Incident Response Implementation Plan and Time Table

Initial Phase

FSA has completed a draft FSA Implementation Guide for the Department's Incident Reporting Procedures and Incident Handling Procedures. This document is currently being reviewed in a draft form by the Department's EDCIRC for compliance and completeness. FSA has been discussing FSA specific issues on incident response with EDCIRC for over four months. The Implementation Guide is tailored for FSA. It takes the Department's recent memorandum and attachment on IT Security Incident Reporting Procedures and also the Department's full-scale Incident Handling Procedures guide (currently only available in draft form) and shows how they will work at FSA.

FSA will make final adjustments to its document once EDCIRC comments are received by 25 April 2003. The document will then be made available for managerial review and approval. After approval we will train the SSOs and system contractors in a formal classroom setting. The incident reporting procedures will be implemented immediately for the initial phase

Final Phase

Implementing the final procedures of the incident response program will not be as easy to accomplish, as it will involve contractual matters. The contractors will be required to report back on the two approaches mentioned in the document. They will be asked to indicate how they intend to implement the requirements, what the impact will be on current procedures and if they foresee additional costs or modifications to current contracts because of these requirements.

The first approach is one in which the contractors all rely upon EDCIRC for all analytical, forensic and remediation services. The contractors will monitor, review logs identify security incidents and suspicious activity and report them as outlined in the guidelines - but that is all.

This is probably the easiest scenario to quickly put into place and will require minor contract modifications to implement. The modifications revolve only around the added requirement of weekly and monthly reports on suspicious activity.

The second of the two possible approaches is one in which the contractors provide for all analytical, forensic and remediation services (using the Departments published standards and guidelines). The contractors will also monitor, review logs identify security incidents and suspicious activity and report them as outlined in the guidelines. EDCIRC will only play a minor supervisory role in this scenario.

This scenario is probably the hardest to quickly put into place as it will place all incident response burdens on the contractor and will definitely be the subject of major contract modification agreements, and will be more expensive to implement.

After the two approaches to incident response are assessed a decision by management will have to be made as to which of the two will be used.

The IT Security Incident Reporting Procedures memorandum has already been sent to the systems contractors. They have been asked to review the memorandum as a preliminary document prior to sending out FSA’s document.

Final Dates

The Department's "Incident Handling Procedures Handbook" is currently going through the approval process. FSA has no control over how long this process will take. The document is one of the primary sources for the Incident Response program. It will provide necessary standards and guidelines. Full implementation cannot proceed until the document is produced.

As mentioned above, it is evident that contractors will ask for modifications to current contracts no matter which final implementation phase is selected. Once again full implementation cannot proceed until this issue is resolved.

With the above caveats in mind, the shown time frames are hard to define and speculative at this time. So much depends on how quickly documents are reviewed and approved and also if any resistance from contractors is encountered. It is reasonable to feel all of this could be implemented by June or July 2003.